Linear Algebra and its Applications **226–228** (1995), 529–551

Two-Graphs and Skew Two-Graphs in Finite Geometries

G. Eric Moorhouse
Dept. of Mathematics, University of Wyoming, Laramie WY, U.S.A.

In honour of Professor J. J. Seidel

Abstract. We describe the use of two-graphs and skew (oriented) two-graphs as isomorphism invariants for translation planes and m-systems (including ovoids and spreads) of polar spaces in odd characteristic.

Keywords: two-graph, polar space, ovoid, spread

1. Introduction

Two-graphs were first introduced by G. Higman, as natural objects for the action of certain sporadic simple groups. They have since been studied extensively by Seidel, Taylor and others, in relation to equiangular lines, strongly regular graphs, and other notions; see [Se1], [Se2], [SeT]. The analogous oriented two-graphs (which we call skew two-graphs) were introduced by Cameron [Cam], and there is some literature on the equivalent notion of switching classes of tournaments.

Our exposition focuses on the use of two-graphs and skew two-graphs as isomorphism invariants of translation planes, and caps, ovoids and spreads of polar spaces in odd characteristic. The earliest precedent for using two-graphs to study ovoids and caps is apparently due to Shult [Sh]. The degree sequences of these two-graphs and skew two-graphs yield the invariants known as fingerprints, introduced by J. H. Conway (see Charnes [Ch1], [Ch2]). Two desirable properties of an isomorphism invariant are that it be

(i) easy or fast to compute, and

(ii) *complete,* i.e. able to distinguish between any two inequivalent examples.

Our two-graphs and skew two-graphs, and their fingerprints, are easily computed in polynomial time. It is not known whether two translation planes of order $n \equiv 1 \mod 4$ with the same two-graph or fingerprint must be equivalent (isomorphic or polar), although for $n \leq 49$ this is true (see Charnes [Ch2], Mathon and Royle [MR], and Section 5). For translation planes of order 27, however, the skew two-graph and fingerprint invariants are not complete (see Dempwolff [D] and Section 5). The question of completeness of two-graph

and fingerprint invariants for ovoids in $O^+_{2r}(q)$ (for q odd) is open for $r \geq 3$, although false for $r = 2$ (Theorem 7.3).

Studies of two-graphs have traditionally emphasised the special class of regular two-graphs. However, most of our two-graphs and skew two-graphs will not be regular. This is fortunate when using two-graphs and skew two-graphs as isomorphism invariants of translation planes or ovoids, since the more varied their degree sequences are, the more successful they will be in distinguishing non-isomorphic objects.

There are several indications that these invariants are natural. They may be constructed both combinatorially (using even vs. odd permutations) and algebraically (using squares vs. nonsquares). Certain infinite families of regular two-graphs and skew two-graphs, including those of Paley, unitary and Ree types, are naturally constructed from ovoids (cf. [Se1]). We also show that two-graphs of caps provide a natural approach to questions in certain geometric settings, including BLT-sets and families of doubly intersecting circles in certain classical circle geometries.

In even characteristic, the two-graph and fingerprint of a translation plane or ovoid is trivial, and so cannot distinguish between any inequivalent examples of the same size. It remains an open problem to find invariants of translation planes and orthogonal ovoids in even characteristic, which are as fast to compute as two-graphs or fingerprints, while being as effective in distinguishing isomorphism types as in odd characteristic.

2. Graphs and Two-Graphs

We summarise here only those definitions and properties of two-graphs required in later sections. For a broader introduction to two-graphs, see [Se1].

Let X be a set of cardinality $v \geq 3$. A *two-graph on* X is a pair (Δ, X) (or simply Δ, if no confusion is likely) where $\Delta \subseteq \binom{X}{3}$ (the set of all 3-subsets of X) such that every 4-subset of X contains an even number (i.e. 0, 2 or 4) of triples from Δ. The *trivial* two-graphs are the *empty two-graph* $\emptyset$ and the *complete two-graph* $\binom{X}{3}$. For any two-graph Δ, its *complement* $\overline{\Delta} := \binom{X}{3} \setminus \Delta$ is also a two-graph. Often we shall be more concerned with the unordered pair $\widetilde{\Delta} := \{\Delta, \overline{\Delta}\}$, which amounts to a partition of $\binom{X}{3}$ into two special subsets. The *degree* of a 2-subset $\{x, y\} \subset X$ is the number of triples $\{x, y, z\} \in \Delta$ containing $\{x, y\}$. We say Δ is *regular* if every 2-subset of X has the same degree; equivalently, when Δ is a 2-$(v, 3, \lambda)$ design for some λ.

Let Γ be an ordinary graph with vertex set X. For each subset $X_1 \subseteq X$, a graph $\Gamma(X_1)$ with vertex set X is obtained from Γ by replacing all edges (respectively, nonedges)

between X_1 and $X \smallsetminus X_1$ with nonedges (resp., edges). Two graphs Γ, Γ' with vertex set X are *switching-equivalent* if $\Gamma' = \Gamma(X_1)$ for some $X_1 \subseteq X$; clearly this is an equivalence relation. The *Seidel adjacency matrix* of Γ, with respect to an ordering $x_1, x_2, \ldots, x_v$ of X, is the $v \times v$ matrix A whose (i,j)-entry is 0 if $i = j$; -1 if x_i is adjacent to x_j, and 1 otherwise. The graph Γ' is switching-equivalent to Γ iff the Seidel adjacency matrix of Γ' equals DAD for some ± 1-diagonal matrix D. Given Γ, define $\Delta(\Gamma)$ to be the collection of all 3-subsets of X which induce an odd number (i.e. 1 or 3) of edges of Γ. Then $\Delta(\Gamma)$ is a two-graph, called the *two-graph of* Γ. Also $\Delta(\Gamma') = \Delta(\Gamma)$ iff Γ' and Γ are switching-equivalent. Clearly $\overline{\Delta}(\Gamma) = \Delta(\overline{\Gamma})$, where $\overline{\Gamma}$ is the complementary graph of Γ.

The *degree sequence* of Δ is the sequence $(n_0, n_1, \ldots, n_{v-2})$ where n_λ is the number of 2-subsets $\{x, y\} \subset X$ of degree λ in Δ. Thus $\sum n_\lambda = v(v-1)/2$, and $\overline{\Delta}$ has degree sequence $(n_{v-2}, n_{v-1}, \ldots, n_0)$. Now let $|AA^\top|$ denote the matrix obtained by replacing each entry of $AA^\top$ by its absolute value. Then the multiset of entries of $|AA^\top|$ is seen to be

$$0^{2n_{r-1}} 2^{2n_{r-2}+2n_r} 4^{2n_{r-3}+2n_{r+1}} \cdots (2r-2)^{2n_0+2n_{2r-2}} (2r-1)^{2r} \quad \text{if } v = 2r, \text{ or}$$

$$1^{2n_{r-1}+2n_r} 3^{2n_{r-2}+2n_{r+1}} 5^{2n_{r-3}+2n_{r+2}} \cdots (2r-1)^{2n_0+2n_{2r-1}} (2r)^{2r+1} \quad \text{if } v = 2r+1.$$

This denotes the fact that 0 occurs $2n_{r-1}$ times in $|AA^\top|$ for $v = 2r$, etc. This multiset clearly depends only on the unordered pair $\widetilde{\Delta} = \{\Delta, \overline{\Delta}\}$. We call this multiset the *fingerprint* of $\overline{\Delta}$ (or of Δ), following Conway, who introduced such invariants for projective planes (see Section 5). We suppress the writing of entries whose frequency is zero; thus for example if Δ is regular of degree k, its fingerprint is $|2k-2r+2|^{2r(2r-1)}(2r-1)^{2r}$ if $v = 2r$, or $|2k-2r+1|^{2r(2r+1)}(2r)^{2r+1}$ if $v = 2r+1$.

3. Tournaments and Skew Two-Graphs

As before, X is a set of cardinality $v \geq 3$. Let $\mathrm{Sym}(X)$ be the group of all permutations of X, and let $\mathcal{T}(X)$ be the set of all 3-cycles in $\mathrm{Sym}(X)$, so that $|\mathcal{T}(X)| = v(v-1)(v-2)/3$. A *skew (oriented) two-graph on* X (cf. [Cam]) is a subset $\nabla \subset \mathcal{T}(X)$ such that

(i) for any $\tau \in \mathcal{T}(X)$, exactly one of τ, τ^{-1} belongs to ∇; and

(ii) for any 4-subset $\{x, y, z, w\} \subseteq X$, ∇ contains an even number (i.e. 0, 2 or 4) of the 3-cycles $(x\,y\,z)$, $(x\,w\,y)$, $(x\,z\,w)$, $(y\,w\,z)$.

(The latter is a conjugacy class of $\mathrm{Alt}\{x, y, z, w\}$.) The *complement* of ∇, $\overline{\nabla} := \mathcal{T}(X) \smallsetminus \nabla = \{\tau^{-1} : \tau \in \nabla\}$ is also a skew two-graph. We denote the unordered pair $\widetilde{\nabla} := \{\nabla, \overline{\nabla}\}$. Unlike the situation for two-graphs, by virtue of property (i) above, there is no 'trivial' skew two-graph. The *degree* of an ordered pair (x, y) (where x, y are distinct elements of

X) is the number or $z \in X$ such that $(x\,y\,z) \in \nabla$. We say that ∇ is *regular* if every pair (x, y) has the same degree (necessarily $(v-2)/2$).

A *tournament on* X is an orientation of the complete graph with vertex set X. If T is a tournament and $X_1 \subseteq X$, a tournament $T(X_1)$ is obtained from T by reversing the orientation of all edges between X_1 and $X \setminus X_1$. We say two tournaments T, T' are *switching-equivalent* if $T' = T(X_1)$ for some $X_1 \subseteq X$. This is an equivalence relation. The $(0, \pm 1)$-*adjacency matrix of* T with respect to an ordering $x_1, \ldots, x_v$ of X, is the $v \times v$ matrix A whose (i, j)-entry is 0 if $i = j$; -1 if $(x_i, x_j) \in T$; and 1 otherwise. We shall also call A a $(0, \pm 1)$-*tournament matrix;* the usual tournament matrix for T is the $(0, 1)$-matrix $\frac{1}{2}(J - I - A)$. A tournament T' is switching-equivalent to T iff the $(0, \pm 1)$-adjacency matrix of T' equals DAD for some ± 1-diagonal matrix D. Define $\nabla(T)$ to be the set of all 3-cycles $(x\,y\,z)$ such that T contains an odd number (i.e. 1 or 3) of the directed edges (x, y), (y, z), (z, x). Then $\nabla(T)$ is a skew two-graph, called the *skew two-graph of* T. Also $\nabla(T') = \nabla(T)$ iff T, T' are switching-equivalent. Clearly, $\overline{\nabla}(T) = \nabla(\overline{T})$ where $\overline{T}$ is the tournament obtained by reversing the orientation of every edge of T. It is easy to see that $\nabla(T)$ is regular iff A is a skew-symmetric conference matrix, iff $A + I$ is a (skew) Hadamard matrix (see [GS], [DGS], [Se1]). In particular, if ∇ is a regular skew two-graph on $v \geq 3$ vertices, then $v \equiv 0 \mod 4$.

If n_λ is the number of ordered pairs (x, y) (where $x \neq y$ in X) of degree λ in ∇, then the degree sequence $(n_0, n_1, \ldots, n_{v-2})$ is palindromic (i.e. $n_\lambda = n_{v-2-\lambda}$) and coincides with the degree sequence of $\overline{\nabla}$. Note that $\sum n_\lambda = v(v-1)$. The multiset of entries of $|AA^\top|$ is

$$0^{n_{r-1}} 2^{2n_{r-2}} 4^{2n_{r-3}} \cdots (2r-2)^{2n_0} (2r-1)^{2r} \quad \text{if } v = 2r, \text{ or}$$
$$1^{2n_{r-1}} 3^{2n_{r-2}} 5^{2n_{r-3}} \cdots (2r-1)^{2n_0} (2r)^{2r+1} \quad \text{if } v = 2r+1.$$

This is an isomorphism invariant of $\widetilde{\nabla} = \{\nabla, \overline{\nabla}\}$, and is called the *fingerprint* of $\widetilde{\nabla}$ (or of ∇).

4. Ovoids and Caps of Polar Spaces.

We refer to Taylor [Ta1] for notation and basic properties of classical groups. For ovoids and spreads of polar spaces, see [Th1], [HT]; however, we differ in that we name polar spaces after the associated groups. Let $\mathcal{P}$ be a classical polar space of rank r in $PG(V) = PG(s, F)$. Then one of the following occurs:

(i) $\mathcal{P}$ is of *orthogonal type* $O^+_{2r}(F)$, $O_{2r+1}(F)$ or $O^-_{2r+2}(F)$ ($s = 2r-1$, $2r$, $2r+1$ respectively). In this case $\mathcal{P}$ is the collection of all subspaces of $PG(V)$ which are totally singular with respect to a particular nondegenerate quadratic form Q on $V = F^{s+1}$, $F = GF(q)$. The associated symmetric bilinear form is $f(x,y) = Q(x+y) - Q(x) - Q(y)$.

(ii) $\mathcal{P}$ is of *unitary type* $U(s+1, F)$, i.e. $\mathcal{P}$ is the collection of all totally isotropic subspaces of V with respect to a nondegenerate Hermitian form f on $V = F^{s+1}$, $F = GF(q^2)$, $r = \lfloor \frac{s+1}{2} \rfloor$.

(iii) $\mathcal{P}$ is of *symplectic type* $Sp(2r, F)$, $s = 2r-1$. Then $\mathcal{P}$ is the collection of all totally isotropic subspaces of V with respect to a nondegenerate alternating bilinear form f on $V = F^{2r}$, $F = GF(q)$.

In the unitary and symplectic cases, a *similarity of* f is a map $g \in GL(V)$ such that $f(x^g, y^g) = \lambda f(x,y)$ for some fixed nonzero $\lambda \in F$; if moreover $\lambda = 1$, then g is an *isometry of* f (called a linear isometry in [Ta1]). In the orthogonal case, similarities and isometries of Q are defined similarly.

Elements of $\mathcal{P}$ have projective dimension $0, 1, \ldots, m, \ldots, r-1$ and are called *points, lines, ..., m-flats, ..., generators.* Let $\mathcal{O}$ be a *k-cap* or *cap of* $\mathcal{P}$, i.e. a collection $\mathcal{O}$ of k points, no two of which are perpendicular (collinear in $\mathcal{P}$). We call $\mathcal{O}$ an *ovoid* if every generator of $\mathcal{P}$ contains a (necessarily unique) point of $\mathcal{O}$. We shall use two equivalence relations for ovoids, namely similarity and isometry. The proof of the following result is straightforward, and is omitted.

4.1 Theorem. *Let $\mathcal{O}$ be a cap in $\mathcal{P}$.*

(i) If $\mathcal{P}$ is of orthogonal or unitary type, or of symplectic type with $q \not\equiv 3 \mod 4$, then the collection of all 3-subsets $\{\langle u\rangle, \langle v\rangle, \langle w\rangle\}$ of $\mathcal{O}$ such that $f(u,v)f(v,w)f(w,u)$ is a nonsquare in F, defines a two-graph $(\Delta(\mathcal{O}), \mathcal{O})$. If q is even, this two-graph is trivial. If $\mathcal{O}'$ is similar (resp., isometric) to $\mathcal{O}$, then $\Delta(\mathcal{O}') \cong \Delta(\mathcal{O})$ or $\overline{\Delta}(\mathcal{O})$ (resp., $\Delta(\mathcal{O}') \cong \Delta(\mathcal{O})$).

(ii) If $\mathcal{P}$ is of symplectic type with $q \equiv 3 \mod 4$, then the collection of all 3-cycles $(\langle u\rangle\ \langle v\rangle\ \langle w\rangle)$ such that $f(u,v)f(v,w)f(w,u)$ is a nonsquare in F, defines a skew two-graph $(\nabla(\mathcal{O}), \mathcal{O})$. If $\mathcal{O}'$ is similar (resp., isometric) to $\mathcal{O}$, then $\nabla(\mathcal{O}') \cong \nabla(\mathcal{O})$ or $\overline{\nabla}(\mathcal{O})$ (resp., $\nabla(\mathcal{O}') \cong \nabla(\mathcal{O})$).

Here it is meaningless to write $\Delta(\mathcal{O}') = \Delta(\mathcal{O})$ since in general these have different point sets. However, by virtue of the above isomorphisms, we speak of $\Delta(\mathcal{O})$ and $\widetilde{\Delta}(\mathcal{O}) =$

$\{\Delta(\mathcal{O}), \overline{\Delta}(\mathcal{O})\}$ (or $\nabla(\mathcal{O})$ and $\widetilde{\nabla}(\mathcal{O}) = \{\nabla(\mathcal{O}), \overline{\nabla}(\mathcal{O})\}$) as *invariants* under the groups of isometries and similarities, respectively. Observe that similar ovoids have the same fingerprint. Fingerprints were used to distinguish several $O_8^+(q)$ ovoids in [Mo].

As a first example, we construct the *Paley two-graphs* Δ_q and the *Paley skew two-graphs* ∇_q from the $Sp(2,q)$ ovoids. Let q be an odd prime power, and let f be a nondegenerate alternating bilinear form on $V = F^2$. The unique ovoid $\mathcal{O}$ consists of all points of the projective line $PG(1,q)$. The isometry group $G = Sp(V,f) = Sp(2,q) \cong SL(2,q)$ acts 2-transitively on $\mathcal{O}$, and has two orbits on ordered triples $(\langle u\rangle, \langle v\rangle, \langle w\rangle)$ of distinct points in $\mathcal{O}$; these orbits are distinguished according to whether or not $f(u,v)f(v,w)f(w,u)$ is a square in F. If $q \equiv 1 \mod 4$, then $\Delta(\mathcal{O}) = \Delta_q := \{\{\langle u\rangle, \langle v\rangle, \langle w\rangle\} : f(u,v)f(v,w)f(w,u)$ is a square in $F\}$ is a regular two-graph of degree $(q-1)/2$, admitting $G/Z(G) \cong PSL(2,q)$. The two-graph isomorphism $\overline{\Delta}_q \cong \Delta_q$ is obtained using a similarity. If $q \equiv 3 \mod 4$, then $\nabla(\mathcal{O}) = \nabla_q := \{(\langle u\rangle\ \langle v\rangle\ \langle w\rangle) : f(u,v)f(v,w)f(w,u)$ is a square in $F\}$ is a regular skew two-graph of degree $(q-1)/2$. Again, $G/Z(G) \cong PSL(2,q)$ acts 2-transitively on ∇_q, and $\overline{\nabla}_q \cong \nabla_q$ by a similarity.

The 2-transitive two-graphs have been classified by Taylor [Ta2]. It is easy to see that the only 2-transitive skew two-graphs are those of Paley type:

4.2 Theorem. *If (∇, X) is a 2-transitive skew two-graph, then X may be identified with $PG(1,q)$ for some $q \equiv 3 \mod 4$, in such a way that $\nabla = \nabla_q$ (of Paley type).*

Proof. Let $G = \mathrm{Aut}(\nabla)$, and let $g \in G$ be an involution. If g fixes a point $x \in X$, then g interchanges two elements $(x\,y\,z)$, $(x\,z\,y) \in \mathcal{T}(X)$, only one of which belongs to ∇, a contradiction. Hence g fixes no point of X. By Bender [Be], there are only two cases to consider. In the first case, $G \geq PSL(2,q)$, $|X| = q+1$ where $q \equiv 3 \mod 4$ and the conclusion follows from the remarks above. In the second case, $G \geq AGL(1,q)$, $|X| = q = 2^e$. Since $AGL(1,4)$ and $PSL(2,3)$ have equivalent actions on 4 points, we may assume that $q \geq 8$, and a contradiction ensues just as in the case of two-graphs; see the proof of Theorem 1 of Taylor [Ta2]. □

The 2-transitive ovoids have been classified by Kleidman [Kl]. Clearly, their associated two-graphs and skew two-graphs are 2-transitive and hence regular, although possibly trivial. In Table 1 we list all 2-transitive ovoids in odd characteristic and having at least three points, and we indicate which of the corresponding two-graphs are trivial.

Ovoid	Restrictions	Nontrivial Δ or ∇?	Description
$Sp(2,q)$	$q \equiv 1 \bmod 4$	nontrivial Δ	Paley Δ_q
$Sp(2,q)$	$q \equiv 3 \bmod 4$	nontrivial ∇	Paley ∇_q
$O_3(q)$	q odd	trivial Δ	Theorem 7.2
$U(3,q)$	q odd	nontrivial Δ	unitary two-graph
$O_4^+(q)$	q odd	trivial Δ	$1+\lfloor \frac{e}{2} \rfloor$ simil. classes
$O_4^-(q)$	q odd	nontrivial Δ	Paley Δ_{q^2}
$O_5(q)$, $O_6^+(q)$	q odd	nontrivial Δ	induced from $O_4^-(q)$
$U(4,q)$	q odd	nontrivial Δ	induced from $U(3,q)$
$O_7(3)$	$q=3$	nontrivial Δ	$Sp(6,2)$
$O_7(q)$	$q=3^e$	nontrivial Δ	$PSU(3,q)$
$O_7(q)$	$q=3^e$, e odd	nontrivial Δ	${}^2G_2(q)$
$O_8^+(q)$	$q=3^e$	nontrivial Δ	induced from $O_7(q)$
$O_8^+(q)$	$q \equiv 2 \bmod 3$	nontrivial Δ	$PSU(3,q)$

TABLE 1

Our construction of the unitary two-graph from the $U(3,q)$ ovoid follows [Se1]. The nontriviality of $\Delta(\mathcal{O})$ for the last four entries, follows from Theorem 7.4; hence by [Ta2], these are the usual unitary and Ree two-graphs. All remaining cases are covered by remarks above and Theorems 7.2 and 7.3.

Suppose $\mathcal{I}(\mathcal{O})$ is an invariant of caps $\mathcal{O}$ which is computed by testing just k-subsets of $\mathcal{O}$, and that the invariant $\mathcal{I}$ is nontrivial (able to distinguish at least two inequivalent caps of the same size). In the orthogonal case, Theorem 4.3 shows that $k \geq 3$, and that if $k=3$, then $\mathcal{I}(\mathcal{O})$ is a function of $\Delta(\mathcal{O})$ and the characteristic is odd. [Note: It is usually possible to define a nontrivial invariant graph $\Gamma(\mathcal{O})$; for example, fix $t \geq 0$ and let $\Gamma(\mathcal{O})$ be the set of pairs $\{\langle u\rangle, \langle v\rangle\}$ in $\mathcal{O}$ such that $|\pi \cap \mathcal{O}| = t$ for some plane π of $PG(V)$ containing $\langle u, v\rangle$. However, the latter definition evidently requires testing subsets of $\mathcal{O}$ of size ≥ 4.] For symplectic polar spaces, however, there are nontrivial triple-based invariants in even characteristic, computed by testing for collinear triples (cf. Theorem 4.4).

4.3 Theorem. *Let $\mathcal{P}$ be an orthogonal polar space in $PG(V) = PG(s,F)$, $s \geq 2$, with associated quadratic form Q on V. Then the number of orbits of $P\Omega(V,Q)$ on ordered 3-caps in $\mathcal{P}$ is*

(i) 1, if q is even and s is odd;

(ii) 2, if q is odd and $\mathcal{P} \neq O^+(4,q)$ (the orbit containing $(\langle u\rangle, \langle v\rangle, \langle w\rangle)$ being determined by whether $f(u,v)f(v,w)f(w,u)$ is a square or a nonsquare in F); or

(iii) 4, if q is odd and $\mathcal{P} = O^+(4,q)$ (as described below).

The number of orbits under $PO(V,Q)$ is 1, 2, 2 respectively.

(Here $O(V,Q)$ is the full linear isometry group, and $\Omega(V,Q)$ is the subgroup defined in [Ta1]. We suppose q and s are not both even; otherwise $\mathcal{P}$ would be a symplectic polar space, which is treated by Theorem 4.4 below.)

Proof. Let $(\langle u\rangle, \langle v\rangle, \langle w\rangle)$, $(\langle u'\rangle, \langle v'\rangle, \langle w'\rangle)$ be two ordered 3-caps in $\mathcal{P}$. Note that $\langle u,v,w\rangle$ and $\langle u',v',w'\rangle$ are nondegenerate planes in $PG(V)$. If $\mathrm{sgn}(f(u,v)f(v,w)f(w,u)) \neq \mathrm{sgn}($ $f(u',v')f(v',w')f(w',u'))$, then clearly the two ordered 3-caps lie in distinct orbits of $PO(V,Q)$.

If q is odd, suppose that $f(u,v)f(v,w)f(w,u)/(f(u',v')f(v',w')f(w',u')) = \alpha^2$ for some $\alpha \in F$; if q is even, then such an α exists automatically. Define a linear transformation $g : \langle u,v,w\rangle \to \langle u',v',w'\rangle$ by

$$u^g = \alpha f(v,w)^{-1} f(v',w')u',$$
$$v^g = \alpha f(w,u)^{-1} f(w',u')v',$$
$$w^g = \alpha f(u,v)^{-1} f(u',v')w'.$$

Then g is an isometry from $\langle u,v,w\rangle$ to $\langle u',v',w'\rangle$. By Witt's Theorem, g extends to an isometry $g \in O(V,Q)$. Moreover, $\langle u^g\rangle = \langle u'\rangle$, $\langle v^g\rangle = \langle v'\rangle$ and $\langle w^g\rangle = \langle w'\rangle$. If $s = 2$ then $PO(V,Q) = P\Omega(V,Q) \cong PSL(2,q)$ and we are done. If $s \geq 4$ then there exists $\sigma \in O(V,Q)$ fixing $\langle u',v',w'\rangle$ pointwise, such that $g\sigma \in \Omega(V,Q)$. Hence we may assume that $s = 3$. Suppose $\mathcal{P} = O^-(4,q)$. If $g \notin \Omega(V,Q)$, we may replace g by $g\rho \in \Omega(V,Q)$ where ρ is a transvection or reflection fixing $\langle u',v',w'\rangle$ pointwise, according as q is even or odd.

This leaves only the case $\mathcal{P} = O^+(4,q)$. If q is even and $g \notin \Omega(V,Q)$, replace g by $g\tau \in \Omega(V,Q)$ where τ is a transvection fixing $\langle u',v',w'\rangle$ pointwise. Hence we may assume q is odd. We may identify $V = V_1 \otimes V_2$ where $V_i \cong F^2$, such that the points $\langle v_1 \otimes v_2\rangle$ of $\mathcal{P}$ are those points of $PG(V)$ represented by the pure tensors $v = v_1 \otimes v_2 \in V$. The symmetric bilinear form satisfies $f(u_1 \otimes u_2,\, v_1 \otimes v_2) = f_1(u_1,v_1)f_2(u_2,v_2)$ where f_i is a nondegenerate alternating form on V_i. Note that $\mathcal{P} \cong \mathcal{P}_1 \times \mathcal{P}_2$ where $\mathcal{P}_i$ is the $Sp(2,q)$-polar space (V_i, f_i), and $P\Omega(V,Q) \cong PSp(2,q) \times PSp(2,q) \leq \mathrm{Aut}(\mathcal{P})$, where the i-th factor $PSp(2,q) \cong PSL(2,q)$ acts on the $q+1$ points of $\mathcal{P}_i$ in the usual way. Therefore two ordered 3-caps $(\langle u\rangle, \langle v\rangle, \langle w\rangle)$ and $(\langle u'\rangle, \langle v'\rangle, \langle w'\rangle)$ are in the same $P\Omega(V,Q)$-orbit

iff $\mathrm{sgn}(f_i(u_i,v_i)f_i(v_i,w_i)f_i(w_i,u_i)) = \mathrm{sgn}(f_i(u_i',v_i')f_i(v_i',w_i')f_i(w_i',u_i'))$ for $i = 1, 2$. There exists $\rho \in O(V,Q) \backslash \Omega(V,Q)$ such that $(v_1 \otimes v_2)^\rho = v_2 \otimes v_1$, which fuses the four $P\Omega(V,Q)$-orbits in pairs, giving two $PO(V,Q)$-orbits. □

4.4 Theorem. *Consider a symplectic polar space $\mathcal{P}$ of type $Sp(2r,q)$ embedded in $PG(V)$ $= PG(2r-1,F)$, with associated alternating bilinear form f on V. Then the number of orbits of $PSp(V,f)$ on ordered 3-caps in $\mathcal{P}$ is*

(i) 1, if q is even and $r = 1$;

(ii) 2, if q is odd and $r = 1$ (the orbit containing $(\langle u\rangle, \langle v\rangle, \langle w\rangle)$ being determined by whether $f(u,v)f(v,w)f(w,u)$ is a square or a nonsquare in F);

(iii) 2, if q is even and $r \geq 2$ (the collinear and noncollinear 3-caps); or

(iv) 4, if q is odd and $r \geq 2$ (collinear with $f(u,v)f(v,w)f(w,u)$ a square or a nonsquare, and noncollinear with $f(u,v)f(v,w)f(w,u)$ a square or a nonsquare).

Proof. It is clear that the number of orbits is at least 1, 2, 2 or 4 respectively. If $r = 1$ then $PSp(V,f) \cong PSL(2,q)$ is 3-transitive for q even, but has two orbits on ordered triples for q odd.

Hence assume $r \geq 2$. For collinear triples, $PSp(V,f)$ induces $PSL(2,q)$ on every hyperbolic line, and the result follows as before. So let $(\langle u\rangle, \langle v\rangle, \langle w\rangle)$ and $(\langle u'\rangle, \langle v'\rangle, \langle w'\rangle)$ be two ordered 3-caps in $\mathcal{P}$, such that $\langle u,v,w\rangle$ and $\langle u',v',w'\rangle$ are planes in $PG(V)$. If q is odd, assume that $f(u,v)f(v,w)f(w,u)/(f(u',v')f(v',w')f(w',u')) = \alpha^2$ for some $\alpha \in F$; if q is even, then such an α exists automatically. Then we construct $g \in Sp(V,f)$ such that $\langle u^g\rangle = \langle u'\rangle$, $\langle v^g\rangle = \langle v'\rangle$ and $\langle w^g\rangle = \langle w'\rangle$, just as in the proof of Theorem 4.3. □

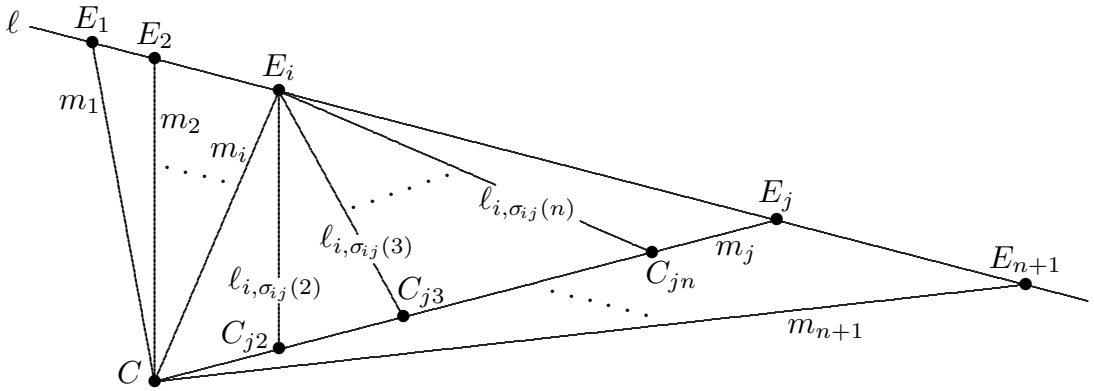
By contrast, for unitary polar spaces, the number of orbits of $PSU(V,f)$ on ordered 3-caps is an unbounded function of V.

5. Invariants of Projective Planes

The following invariants of finite projective planes, due to J. H. Conway, are described in [Ch1], [Ch2].

Let Π be a projective plane of order n, and let (C,ℓ) be an *antiflag* (nonincident point-line pair) in Π. Label the points on ℓ as $E_1, E_2, \ldots, E_{n+1}$; then the lines through C are

$m_i := CE_i,\ i = 1, 2, \ldots, n+1$. Label the points on m_i as $C_{i,1}$=C, $C_{i,2}$, ..., $C_{i,n+1}$=E_i. Dually, label the lines through E_i as $\ell_{i,1}$=ℓ, $\ell_{i,2}$, ..., $\ell_{i,n+1}$=m_i.



Now let $i \neq j$. Each point $C_{j,k}$ lies on a unique line $\ell_{i,\sigma_{ij}(k)}$ through E_i, for some permutation $\sigma_{ij} \in S_{n+1}$. Define the *sign matrix* A to be the $(n+1) \times (n+1)$ matrix whose (i,j)-entry is $\mathrm{sgn}(\sigma_{ij})$; also the (i,i)-entry of A is 0. A change of labels has the effect of replacing A by an *equivalent* sign matrix $A' = DPAP^\top D'$ for some permutation matrix P and ± 1-diagonal matrices D, D'. Therefore the matrix $AA^\top$ (computed in characteristic zero) depends on the triple (Π, C, ℓ) only to within conjugation by a ± 1-*monomial matrix* (i.e. a product DP as above). The *fingerprint* of (Π, C, ℓ) is the multiset of all entries in $|AA^\top|$, in the notation of Section 2. Here the term 'fingerprint' is applied in a more general setting than in Sections 2 and 3, since A need not be equivalent to either a symmetric or skew-symmetric matrix (we have shown this for certain antiflags in the Hughes plane of order 9). Clearly, the fingerprint is an isomorphism invariant of the triple (Π, C, ℓ). (A variation of the above, using square matrices of size $n^2 + n + 1$, gives an invariant of Π itself; see [Ch2].)

The fingerprint of (Π, C, ℓ) is most useful when Π has a canonical choice of antiflag (C, ℓ), so that the fingerprint depends only on Π. For example, if Π is a translation plane, we define the fingerprint of Π to be the fingerprint of (Π, O, ℓ_∞) where ℓ_∞ is the line at infinity, and O is any affine point. Since any finite non-Desarguesian translation plane has a unique translation line ℓ_∞ and the affine points are equivalent under the translation group, it follows that isomorphic translation planes have the same fingerprint. Moreover, we will show (Theorem 5.2) that in the case Π is a translation plane, the sign matrix A is equivalent to a symmetric or skew-symmetric matrix; this gives a complementary pair of two-graphs $\widetilde{\Delta}(\Pi)$ or of skew two-graphs $\widetilde{\nabla}(\Pi)$ whose fingerprint is that of Π. (This fails for more general triples (Π, C, ℓ), as mentioned above.) We require:

5.1 Lemma. *Let $M \in GL(r,F)$, $r \geq 1$, $F = GF(q)$. Let σ and ρ be the permutations induced by M on the vectors, and on the one-dimensional subspaces of V, respectively. Then* $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\det M)$ *and* $\mathrm{sgn}(\rho) = (\mathrm{sgn}(\det M))^{r-1}$.

Proof. Assume that $(r,q) \neq (2,2)$, so that $SL(r,F)$ is the derived subgroup of $G := GL(r,F)$. (The case $GL(2,2)$ is trivial.) Clearly the result follows for $M \in SL(r,F)$. Now choose $M_{q^r-1} \in G$ which acts regularly on the nonzero vectors in F^r. Then $\det(M_{q^r-1})$ is a generator of the multiplicative group of $F \setminus \{0\}$, so $\mathrm{sgn}(\det(M_{q^r-1})) = \pm 1$ where the upper (lower) sign is chosen for q even (odd). Also in this case, σ is a (q^r-1)-cycle and ρ is a $(q^{r-1}+\cdots+q+1)$-cycle, so that $\mathrm{sgn}(\sigma) = \pm 1$ and $\mathrm{sgn}(\rho) = (\pm 1)^{r-1}$. Since $G = \langle SL(r,F), M_{q^r-1} \rangle$, the result follows. □

Let $\{M_1, M_2, \ldots, M_{q^r}\}$ be a spread set for a translation plane Π of order q^r with kernel containing $GF(q)$ (see [L]). Thus M_i is an $r \times r$ matrix over $GF(q)$ and $M_i - M_j$ is nonsingular whenever $i \neq j$. Now Π has $V \oplus V$ as its set of affine points, where $V = F^r$, and its affine lines are the subsets $\{(x, xM_i + b) : x \in V\}$ for $b \in V$, $i = 1, 2, \ldots, q^r$ (the lines "$y = xM_i + b$"), and $\{(a,y) : y \in V\}$ for $a \in V$ (the lines "$x = a$"). Define $\mathrm{sgn} : F \to \{-1, 0, 1\}$ by

$$\mathrm{sgn}(a) = \begin{cases} 0, & a = 0; \\ 1, & a \text{ is a nonzero square in } F; \\ -1, & \text{otherwise.} \end{cases}$$

(Note that $\mathrm{sgn}(a) \in \{0,1\}$ if q is even.) Let $\widehat{A}$ be the $q^r \times q^r$ matrix whose (i,j)-entry is $\mathrm{sgn}(\det(M_j - M_i))$.

5.2 Theorem. *Let A be the sign matrix of (Π, O, ℓ_∞).*

(i) If $q^r \not\equiv 3 \pmod 4$, then A is equivalent to the symmetric matrix $\begin{bmatrix} \widehat{A} & \mathbf{1}^\top \\ \mathbf{1} & 0 \end{bmatrix}$, which is the Seidel adjacency matrix of a graph Γ. Moreover, the pair $\widetilde{\Delta}(\Pi) := \{\Delta(\Gamma), \overline{\Delta}(\Gamma)\}$ depends only on the isomorphism class of Π. If q is even, the pair $\widetilde{\Delta}(\Pi)$ is trivial.

(ii) If $q^r \equiv 3 \pmod 4$, then A is equivalent to the skew-symmetric matrix $\begin{bmatrix} \widehat{A} & \mathbf{1}^\top \\ -\mathbf{1} & 0 \end{bmatrix}$, which is the $(0, \pm 1)$-adjacency matrix of a tournament T. Moreover, the pair $\widetilde{\nabla}(\Pi) := \{\nabla(T), \overline{\nabla}(T)\}$ depends only on the isomorphism class of Π.

Proof. Let $v_1 = 0, v_2, v_3, \ldots, v_n$ be the $n = q^r$ vectors in V. We label the lines of Π in accordance with our earlier labelling, as follows, where $1 \leq i, j \leq n$. The lines of Π are $\ell = \ell_\infty$, ℓ_{ij} (the line "$y = xM_i + v_j$"; this includes $m_i = \ell_{i1}$, the line "$y = xM_i$"),

and $\ell_{n+1,j}$ (the line "$x = v_j$"). The points of Π are $C = O = (0,0)$, $E_j = m_j \cap \ell_\infty$, $C_{ij} = (v_j, v_j M_i)$, and $C_{n+1,j} = (0, v_j)$ (so that $C_{i1} = C_{n+1,1} = O$). From the definitions, we see that $v_{\sigma_{ij}(k)} = v_k(M_j - M_i)$ for $i \neq j$, and $\sigma_{i,n+1}(k) = \sigma_{n+1,j}(k) = k$. By Lemma 5.1, $\mathrm{sgn}(\sigma_{ij}) = \mathrm{sgn}(\det(M_j - M_i))$ for $i \neq j$, and $\mathrm{sgn}(\sigma_{i,n+1}) = \mathrm{sgn}(\sigma_{n+1,j}) = 1$. This gives $\left[\begin{smallmatrix} \widehat{A} & \mathbf{1}^\top \\ \mathbf{1} & 0 \end{smallmatrix}\right]$ for the sign matrix, where $\widehat{A}$ is as above. If $q^r \not\equiv 3 \mod 4$, then $\det(M_j - M_i) = (-1)^r \det(M_i - M_j)$ where $(-1)^r$ is a square in F, so that $\widehat{A}$ is symmetric and conclusion (i) follows from previous discussion. If $q^r \equiv 3 \mod 4$, then $\det(M_j - M_i) = -\det(M_i - M_j)$ where $-1 \in F$ is a nonsquare, so that $\widehat{A}$ is skew-symmetric. Multiplying the last row of $\left[\begin{smallmatrix} \widehat{A} & \mathbf{1}^\top \\ \mathbf{1} & 0 \end{smallmatrix}\right]$ by -1 gives a sign matrix equivalent to A, and conclusion (ii) follows. □

Given a translation plane Π with spread set $\{M_i\}$, then the transposed matrices $\{M_i^\top\}$ form a spread set for a translation plane Π^*, called the *polar translation plane of* Π. Viewing Π as a spread of $PG(2r-1, q)$, then Π^* is the image of Π under a polarity of $PG(2r-1, q)$. If $\Pi^* \cong \Pi$, we say Π is *self-polar;* otherwise, $\{\Pi, \Pi^*\}$ is a *polar pair.* By Theorem 5.2, Π and Π^* yield the same $\widetilde{\Delta}$ or the same $\widetilde{\nabla}$, according as $q \not\equiv 3$ or $q \equiv 3 \mod 4$. It is not known whether two translation planes of order $q \equiv 1 \mod 4$ with the same fingerprint must be either isomorphic or polar, although for $q \leq 49$ this is the case. However, there do exist nonisomorphic (and non-polar) translation planes of order 27 with isomorphic skew two-graphs. We proceed to describe the cases $q \leq 49$.

There are precisely two translation planes of order 9, namely $AG(2,9)$ and $Hall(9)$. We have $\widetilde{\Delta}(AG(2,9)) = \{\Delta_{\mathrm{Pet}}, \overline{\Delta}_{\mathrm{Pet}}\}$ where $\Delta_{\mathrm{Pet}} \cong \overline{\Delta}_{\mathrm{Pet}}$ corresponds to the switching class of the Petersen graph, is regular of degree 4, and has fingerprint $0^{90}9^{10}$. However, $\widetilde{\Delta}(Hall(9)) = \{\Delta_{\mathrm{Hall}}, \overline{\Delta}_{\mathrm{Hall}}\}$, where Δ_{Hall} has (n_2=40, n_8=5) and corresponds to the switching class of the graph  , with fingerprint $2^{80}8^{10}9^{10}$.

There are exactly 21 isomorphism types of translation planes of order 25, including one polar pair and 19 self-polar planes; see Czerwinski and Oakden [CO], [Cz]. From this list, Charnes [Ch2] has determined that two translation planes of order 25 with the same fingerprint are necessarily either isomorphic or polar. A similar conclusion holds for the translation planes of order 49, of which there are 1347 isomorphism types, including 374 polar pairs and 599 self-polar classes; see Mathon and Royle [MR].

The situation for translation planes of order 3 modulo 4 seems to be quite different. Dempwolff [D] has shown that there are exactly 7 isomorphism classes of translation planes of order 27, each of which is self-polar. Three of these (Desarguesian (I), a generalised

twisted field plane (II), and a flag transitive plane (IV)) have the same fingerprint, while the remaining four fingerprints are distinct. Using the graph isomorphism package `nauty` [Mc], we have found that the planes (I), (II) and (IV) in fact have isomorphic skew two-graphs; this is the Paley skew two-graph ∇_{27}. Dempwolff's classification [D] uses a new isomorphism invariant, his *Kennvector,* which is a complete invariant for translation planes of order 27, but is more expensive to compute than the fingerprint.

5.3 Theorem. *Let $\mathcal{O}$ be an ovoid in $O_6^+(q)$, and let Π be the translation plane constructed from $\mathcal{O}$ by the Klein correspondence, as in [Ka1]. Then $\widetilde{\Delta}(\mathcal{O}) \cong \widetilde{\Delta}(\Pi)$.*

Proof. We may assume that $Q(x) = x_0x_5 + x_1x_4 + x_2x_3$ and $\mathcal{O} = \{\langle v_\infty\rangle\} \cup \{\langle v_i\rangle : i = 0, 1, \ldots, q^2-1\}$ where $v_\infty = (000001)$ and $v_i = (1, a_i, b_i, c_i, -d_i, a_id_i - b_ic_i)$. Then the matrices $M_i = \left[\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right]$ form a spread set for Π, and $f(v_i, v_j) = \det(M_i - M_j)$, $f(v_i, v_\infty) = 1$. The result follows from Theorem 5.2. □

Note that the polarity $M_i \mapsto M_i^\top$ of translation planes is induced by the isometry $x \mapsto (x_0, x_1, x_3, x_2, x_4, x_5)$ in $PO_6^+(q) \backsim P\Omega_6^+(q)$.

6. Spreads and m-Systems of Polar Spaces.

Let $\mathcal{P}$ be a polar space of rank r, as in Section 4. The following generalisation of ovoids and spreads is due to Shult and Thas [ShT]. A *partial m-system* of $\mathcal{P}$ is a collection $\mathcal{M} = \{\pi_1, \ldots, \pi_k\}$ of m-flats of $\mathcal{P}$ such that $\pi_i^\perp \cap \pi_j = \emptyset$ for all $i \neq j$.

6.1 Theorem [ShT]**.** *For any partial m-system $\mathcal{M}$ in $\mathcal{P}$,*

$$|\mathcal{M}| \leq \begin{cases} q^{r-1}+1, & \mathcal{P} = O_{2r}^+(q); \\ q^r+1, & \mathcal{P} = O_{2r+1}(q) \text{ or } Sp(2r,q); \\ q^{r+1}+1, & \mathcal{P} = O_{2r+2}^-(q); \\ q^{2r-1}+1, & \mathcal{P} = U(2r, q^2); \\ q^{2r+1}+1, & \mathcal{P} = U(2r+1, q^2). \end{cases}$$

If $|\mathcal{M}|$ attains the upper bound of Theorem 6.1, $\mathcal{M}$ is called an *m-system.* A 0-system is the same as an *ovoid*; a partial 0-system is a *cap*; and an $(r-1)$-system is a *spread* of $\mathcal{P}$, i.e. a collection of generators which partition the point set of $\mathcal{P}$.

Let π, π' be two m-flats of $\mathcal{P}$, where $0 \leq m \leq r-1$, and let $\{v_1, \ldots, v_{m+1}\}$, $\{v_1', \ldots, v_{m+1}'\}$ be bases of the corresponding subspaces of V. Define

$$\mathrm{sgn}(\pi,\pi') := \mathrm{sgn}\big[\det\big(f(v_i,v'_j)\ :\ 1\le i,j\le m{+}1\big)\big].$$

Note that $\mathrm{sgn}(\pi,\pi') \in \{-1,0,1\}$ is well-defined, and $\mathrm{sgn}(\pi,\pi') \neq 0$ iff $\pi^\perp \cap \pi' = \emptyset$. We have the following easy generalisation of Theorem 4.1:

6.2 Theorem. *Let $\mathcal{M}$ be an m-system or partial m-system in $\mathcal{P}$.*

(i) Suppose $\mathcal{P}$ is of orthogonal or unitary type, or of symplectic type with $q^{m+1} \not\equiv 3$ mod 4. Then the collection of all 3-subsets $\{\pi,\pi',\pi''\}$ of $\mathcal{M}$ such that $\mathrm{sgn}(\pi,\pi')\mathrm{sgn}(\pi',\pi'')\mathrm{sgn}(\pi'',\pi) = -1$, defines a two-graph $(\Delta(\mathcal{M}),\mathcal{M})$. If q is even, this two-graph is empty.

(ii) Suppose $\mathcal{P}$ is of symplectic type with $q^{m+1} \equiv 3$ mod 4. Then the collection of all 3-cycles $(\pi\,\pi'\,\pi'') \in \mathcal{T}(\mathcal{M})$ such that $\mathrm{sgn}(\pi,\pi')\mathrm{sgn}(\pi',\pi'')\mathrm{sgn}(\pi'',\pi) = -1$, defines a skew two-graph $(\nabla(\mathcal{M}),\mathcal{M})$.

The associated two-graph or skew two-graph is invariant under isometries. The associated pair $\widetilde{\Delta} = \{\Delta,\overline{\Delta}\}$ or $\widetilde{\nabla} = \{\nabla,\overline{\nabla}\}$, and the fingerprint, are invariant under similarities.

Alternative definitions of the above two-graphs and skew two-graphs are possible, in the combinatorial spirit of Conway's description for planes (Section 5); we present just one as an example. Let $\mathcal{P}$ be an $Sp(4,q)$ polar space (generalised quadrangle). For each line of $\mathcal{P}$, choose an ordering of its $q+1$ points. Let ℓ,ℓ' be two disjoint lines of $\mathcal{P}$, whose points have been numbered (say) P_i, P'_i, $i = 1,2,\ldots,q+1$. Each point $P'_i \in \ell'$ is collinear in $\mathcal{P}$ (i.e. perpendicular) to a unique point $P_{\sigma_{\ell,\ell'}(i)} \in \ell$, where $\sigma_{\ell,\ell'} \in S_{q+1}$. Now suppose $\mathcal{M}$ is a partial spread of $\mathcal{P}$, i.e. a collection of mutually disjoint lines, $|\mathcal{M}| \le q^2+1$. Clearly, the collection of all 3-subsets $\{\ell,\ell',\ell''\}$ of $\mathcal{M}$ such that $\mathrm{sgn}(\sigma_{\ell,\ell'}\sigma_{\ell',\ell''}\sigma_{\ell'',\ell}) = -1$ defines a two-graph $\Delta_{\mathrm{Comb}}(\mathcal{M})$, independent of the above choice of ordering of points.

6.3 Theorem. *To within complementation, the two-graphs $\Delta_{\mathrm{Comb}}(\mathcal{M})$, $\Delta(\mathcal{M})$ and $\Delta(\mathcal{O})$ coincide, where $\mathcal{O}$ is a cap of $O_5(q)$ identified with $\mathcal{M}$ by a duality. In particular, all these two-graphs have the same fingerprint.*

Proof. We may suppose q is odd. Consider triples $\{\ell,\ell',\ell''\}$ consisting of three mutually disjoint lines of $\mathcal{P}$. Let S^ϵ be the collection of such triples for which $\mathrm{sgn}(\ell,\ell')\mathrm{sgn}(\ell',\ell'')\mathrm{sgn}(\ell'',\ell) = \epsilon$, and let $S^\epsilon_{\mathrm{Comb}}$ be the collection of such triples for which $\mathrm{sgn}(\sigma_{\ell,\ell'}\sigma_{\ell',\ell''}\sigma_{\ell'',\ell}) = \epsilon$. Clearly each of the collections $S^+, S^-, S^+_{\mathrm{Comb}}, S^-_{\mathrm{Comb}}$ is invariant under $PSp(4,q)$, and by explicit calculation, each of these collections is nonempty. Therefore both partitions

$S^+ \cup S^-$ and $S^+_{\rm Comb} \cup S^-_{\rm Comb}$ must correspond, under duality, to the partition of 3-caps of $O_5(q)$ given by Theorem 4.3(ii). The result follows. □

Further theorems showing equivalence of combinatorial and algebraic constructions of two-graph invariants, and showing their invariance under under dualities and trialities, are possible.

7. Caps whose Two-Graphs are Trivial

It is often of interest to consider consider caps $\mathcal{O}$ in polar spaces for which $|\mathcal{O}|$ is maximal subject to $\Delta(\mathcal{O})$ being trivial. For example, let q be odd, and let $\mathcal{O}$ be a collection of singular points in $O_5(q)$ such that $\langle u,v,w\rangle^\perp$ is an elliptic (i.e. anisotropic) line for all distinct $\langle u\rangle$, $\langle v\rangle$, $\langle w\rangle$ in $\mathcal{O}$. Then $|\mathcal{O}| \le q+1$, and if equality holds, $\mathcal{O}$ is called a *BLT-set* (see Bader, Lunardon and Thas [BLT], Kantor [Ka3]). A flock of a quadratic cone in $PG(3,q)$ is equivalent to a pair $(\mathcal{O},\langle u\rangle)$ consisting of a BLT-set $\mathcal{O}$ and a distinguished point $\langle u\rangle \in \mathcal{O}$. We observe that BLT-sets may be considered as maximal caps with trivial two-graphs:

7.1 Theorem. *Let Q be a nondegenerate quadratic form on $V = F^5$ with discriminant δ, where $F = GF(q)$, q odd. Suppose $\mathcal{O}$ is a cap in the polar space $\mathcal{P} = \mathcal{P}(V,Q)$ of type $O_5(q)$. Then*

(i) if $\Delta(\mathcal{O})$ is complete and -2δ is a square in F, then $|\mathcal{O}| \le q+1$;
(ii) if $\Delta(\mathcal{O})$ is empty and -2δ is a nonsquare in F, then $|\mathcal{O}| \le q+1$.

Moreover, $\mathcal{O}$ is a BLT-set in $\mathcal{P}$ iff equality holds in (i) or in (ii).

Proof. It suffices to show that if $\langle u\rangle$, $\langle v\rangle$, $\langle w\rangle$ are three singular points, then $\langle u,v,w\rangle^\perp$ is an elliptic line iff $-2\delta f(u,v)f(v,w)f(w,u)$ is a nonsquare in F, where $f(x,y) = Q(x+y) - Q(x) - Q(y)$. To see this, suppose that u,v,w are linearly independent, and let $\{x,y\}$ be a basis for $\langle u,v,w\rangle^\perp$. Computing the discriminant of Q with respect to the basis $\{u,v,w,x,y\}$ of V, we see that $a^2\delta = 2f(u,v)f(v,w)f(w,u)\mathrm{disc}\big(Q|_{\langle x,y\rangle}\big)$ where $a \ne 0$; furthermore, the line $\langle x,y\rangle$ is elliptic iff $-\mathrm{disc}\big(Q|_{\langle x,y\rangle}\big)$ is a nonsquare in F. The result follows. □

Now suppose $\mathcal{O}$ is any cap contained in a hyperplane of $O_5(q)$, such that $\Delta(\mathcal{O})$ is trivial. One may show that $|\mathcal{O}| \le q+1$ by Theorem 7.1; better yet, it is possible to

characterise those cases for which equality occurs, using parallel results of Blokhuis [Bl] and Carlitz [Car]. It may be seen that these results rephrase two theorems of Thas [Th2] concerning flocks whose planes share a common point.

7.2 Theorem (cf. Thas [Th2]). *Let $\mathcal{O}$ be a $(q+1)$-cap in $O_4^-(q)$, where q is odd. Then $\Delta(\mathcal{O})$ is trivial if and only if $\mathcal{O}$ is a conic.*

Proof. Suppose $\mathcal{O}$ is a conic. For any 3-subset $\{\langle u\rangle, \langle v\rangle, \langle w\rangle\}$ of $\mathcal{O}$, we may compute the discriminant of $\langle\mathcal{O}\rangle$ as $\delta = 2f(u,v)f(v,w)f(w,u)$, so $\Delta(\mathcal{O})$ is either empty or complete, according as 2δ is a square or a nonsquare.

To prove the converse, we may suppose that $Q(x) = x_0x_1 - x_2^2 + \varepsilon x_3^2$ and $\mathcal{O} = \{\langle(0,1,0,0)\rangle\} \cup \{\langle(1,\, \alpha_i^2 - \varepsilon\beta_i^2,\, \alpha_i,\, \beta_i)\rangle \,:\, 1 \le i \le q\}$ where $\varepsilon \in F$ is a fixed nonsquare. If $\Delta(\mathcal{O})$ is trivial, then for all $i \ne j$, the expression $(\alpha_i - \alpha_j)^2 - \varepsilon(\beta_i - \beta_j)^2$ is either always a nonzero square, or always a nonsquare, in F. Consider a quadratic extension $E = F(\theta)$ where $\theta^2 = \varepsilon$. For $x, y \in F$, the element $x + \theta y$ is a square in E iff its norm, $x^2 - \varepsilon y^2$, is a square in F. Therefore the differences of the elements $\alpha_i + \theta\beta_i$ are always squares, or always nonsquares in E. By [Bl], there exist $a, b, c \in F$, where $(a,b) \ne (0,0)$, such that $a\alpha_i + b\beta_i + c = 0$ for all i. Then $\mathcal{O}$ consists of all singular points in the plane $cx_0 + ax_2 + bx_3 = 0$. □

Next we classify those $(q+1)$-caps (i.e. ovoids) in $O_4^+(q)$ with trivial two-graphs. Let $\mathcal{P}$ be the hyperbolic quadric $x_0x_3 - x_1x_2 = 0$ in $PG(3,q)$, $q = p^e$ odd. Then $\mathcal{P}$ has $(q+1)!$ ovoids, these being the transversals of a $(q+1) \times (q+1)$ grid. Every such ovoid is isometric to one of the form $\mathcal{O}(\pi) = \{\langle v_\infty\rangle\} \cup \{\langle v_t\rangle \,:\, t \in F\}$ where $v_\infty = (0,0,0,1)$ and $v_t = (1, t, t^\pi, tt^\pi)$ for some permutation $\pi : F \to F$. In particular, for the identity permutation $\iota : F \to F$, the ovoid $\mathcal{O}(\iota)$ is a conic, i.e. a nondegenerate plane section of $\mathcal{P}$. More generally, Kleidman [Kl] has shown that the 2-transitive ovoids of $\mathcal{P}$ are precisely the ovoids similar to $\mathcal{O}(\sigma)$ for some $\sigma \in \mathrm{Aut}(F)$; furthermore, two 2-transitive ovoids $\mathcal{O}(\sigma')$, $\mathcal{O}(\sigma)$ are similar iff $\sigma' = \sigma^{\pm 1}$. Thus $\mathcal{P}$ has precisely $\lfloor \frac{e}{2} \rfloor + 1$ similarity classes of 2-transitive ovoids.

We have $f(v_\infty, v_t) = 1$ and $f(v_s, v_t) = (s-t)(s^\pi - t^\pi)$ for all $s, t \in F$. Therefore $\Delta(\mathcal{O}(\pi))$ is trivial iff $(s-t)(s^\pi - t^\pi)$ is a nonzero square for all $s \ne t$ in F. By [Car], this occurs iff $t^\pi = a^2t^\sigma + b$ for some $\sigma \in \mathrm{Aut}(F),\ a, b \in F,\ a \ne 0$. We may assume that $a = 1$

and $b=0$, since the isometry $(x_0,x_1,x_2,x_3) \mapsto (ax_0,\, ax_1,\, a^{-1}(x_2-bx_0),\, a^{-1}(x_3-bx_0))$ maps $\mathcal{O}(\pi)$ to $\mathcal{O}(\sigma)$. We have shown the following:

7.3 Theorem (cf. Thas [Th2]). *Let $\mathcal{O}$ be an ovoid in $O_4^+(q)$, where q is odd. Then $\Delta(\mathcal{O})$ is trivial iff $\mathcal{O}$ is 2-transitive, iff $\mathcal{O}$ is similar to $\mathcal{O}(\sigma)$ for some $\sigma \in \mathrm{Aut}(F)$.*

It is known (see [BLT]) that when $\mathcal{O}$ is a conic, the corresponding flocks are linear; when $\mathcal{O}$ is one of the nonlinear examples of Theorem 7.3, the corresponding flocks arise from a family of Kantor [Ka2].

For more general polar spaces, we will obtain the following weaker bound for caps with trivial two-graphs.

7.4 Theorem. *Let $\mathcal{P}$ be a polar space naturally embedded in $PG(n,q)$, where $q=p^e$ is odd. If $\mathcal{O}$ is a cap in $\mathcal{P}$ whose two-graph $\Delta(\mathcal{O})$ is trivial, then $|\mathcal{O}| \le \binom{n+(p-1)/2}{n}^e + 1$.*

The latter bound is a consequence of the following. Let $\mathcal{S}$ be a set of $s := (q^{n+1}-1)/(q-1)$ vectors in $V=F^{n+1}$, which represent the s distinct points of $PG(n,F)$, $F=GF(q)$, $q=p^e$. Let M be the $s\times s$ matrix with entries $m_{x,y} := (x_0y_0+\cdots+x_ny_n)^{(q-1)/2}$ where $x=(x_0,\ldots,x_n)$, $y=(y_0,\ldots,y_n)\in\mathcal{S}$.

7.5 Lemma. *The matrix M has rank $\binom{n+(p-1)/2}{n}^e$ over F.*

Proof. Suppose $v=\big(v_y \,:\, y\in\mathcal{S}\big)$ is in the right null space of M. Then for all $x\in\mathcal{S}$,

$$\begin{aligned} 0 &= \sum_{y\in\mathcal{S}} m_{x,y}v_y = \sum_{y\in\mathcal{S}} (x_0y_0+\cdots+x_ny_n)^{(q-1)/2}v_y \\ &= \sum_{y\in\mathcal{S}} \sum_{i_0,\ldots,i_n} \binom{(q-1)/2}{i_0,\, i_1,\, \ldots,\, i_n} x_0^{i_0}y_0^{i_0}x_1^{i_1}y_1^{i_1}\cdots x_n^{i_n}y_n^{i_n}v_y \\ &= \sum_{i_0,\ldots,i_n} \binom{(q-1)/2}{i_0,\, i_1,\, \ldots,\, i_n} \Big[\sum_{y\in\mathcal{S}} y_0^{i_0}y_1^{i_1}\cdots y_n^{i_n}v_y\Big] x_0^{i_0}x_1^{i_1}\cdots x_n^{i_n} \end{aligned}$$

where $\binom{(q-1)/2}{i_0,\,i_1,\,\ldots,\,i_n} := \frac{((q-1)/2)!}{i_0!i_1!\cdots i_n!}$ and $i_0,i_1,\ldots,i_n$ are non-negative integers summing to $(q-1)/2$. By Lemma 2.3 of [BM], this implies that for all such $(i_0,i_1,\ldots,i_n)$, we have

$$0 = \binom{(q-1)/2}{i_0,\, i_1,\, \ldots,\, i_n} \sum_{y\in\mathcal{S}} y_0^{i_0}y_1^{i_1}\cdots y_n^{i_n}v_y\,.$$

Consider the p-ary expansions $i_j = \sum_{k=0}^{e-1} i_{j,k} p^k$ where $0 \le i_{j,k} < p$, and $\frac{q-1}{2} = \sum_{k=0}^{e-1} \frac{p-1}{2} p^k$. Then by Lucas' Theorem (cf. [BW]) we have

$$\binom{(q-1)/2}{i_0,\, i_1,\, \ldots,\, i_n} \equiv \prod_{k=0}^{e-1} \binom{(p-1)/2}{i_{0,k},\, i_{1,k},\, \cdots,\, i_{n,k}} \mod p\,.$$

Thus $p \not| \binom{(q-1)/2}{i_0,\, i_1,\, \ldots,\, i_n}$ iff $\sum_{k=0}^{e-1} i_{j,k} = (p-1)/2$ for all $j = 0, 1, \ldots, n$. The number of $(i_0, i_1, \ldots, i_n)$ satisfying this condition is $\binom{n+(p-1)/2}{n}^e$. We therefore have $\binom{n+(p-1)/2}{n}^e$ linear conditions

$$0 = \sum_{p \not| \binom{(p-1)/2}{i_0,\, i_1,\, \ldots,\, i_n}} y_0^{i_0} y_1^{i_1} \cdots y_n^{i_n} v_y\,.$$

The coefficient matrix in the latter linear system has full rank by Lemma 2.3 of [BM], so the null space of M over F has dimension $s - \binom{n+(p-1)/2}{n}^e$. Thus $\operatorname{rank}_F M = s - \left[s - \binom{n+(p-1)/2}{n}^e\right] = \binom{n+(p-1)/2}{n}^e$. □

Proof of Theorem 7.4. Let δ be the polarity of $PG(V)$ corresponding to $\mathcal{P}$. Let $v_1, \ldots, v_k$ be vectors in $V = F^{n+1}$ representing the points of $\mathcal{O}$. We have $v_i = (v_{i0}, \ldots, v_{in})$. Choose a linear equation $\sum_{t=0}^{n} u_{i,t} X_t = 0$ for the polar hyperplane v_i^δ. Let A be the $k \times k$ matrix with entries

$$a_{ij} = \Big(\sum_{t=0}^{n} u_{it} v_{jt}\Big)^{(q-1)/2} = \begin{cases} 0, & i = j; \\ 1, & i \ne j \text{ and } \sum_t u_{it} v_{jt} \text{ is a square;} \\ -1, & i \ne j \text{ and } \sum_t u_{it} v_{jt} \text{ is a nonsquare.} \end{cases}$$

Then A is the Seidel adjacency matrix of a graph in the switching class corresponding to $\Delta(\mathcal{O})$. Note that $\operatorname{rank}_F A$ depends only on the switching class of A, and hence only on $\Delta(\mathcal{O})$. If $\Delta(\mathcal{O})$ is trivial, we may assume that $A = J - I$, and so $\operatorname{rank}_F A \ge k - 1$. Furthermore, A is switching-equivalent to a submatrix of the matrix M defined above, and so by Lemma 7.5, $|\mathcal{O}| = k \le 1 + \operatorname{rank}_F A \le 1 + \operatorname{rank}_F M = 1 + \binom{n+(p-1)/2}{n}^e$. □

Note that Theorem 7.4 can be improved slightly in some cases, since $\operatorname{rank}_F(J - I) = k$ whenever $k \not\equiv 1 \mod p$. For example, this gives $|\mathcal{O}| \le \binom{n+(p-1)/2}{n}^e$ whenever $n \le (p-1)/2$.

8. Intersecting Circles in Laguerre Planes

Let $\mathfrak{M} = (\mathfrak{P}, \mathfrak{C})$ be a classical Laguerre plane of odd order q. Thus $\mathfrak{M}$ is an incidence system having point set $\mathfrak{P}$ consisting of the $q(q+1)$ points of a quadratic cone in $PG(3, q)$

distinct from the vertex, and set $\mathfrak{C}$ of blocks ('circles') consisting of the conics which are plane sections of the cone. A *family of doubly intersecting circles in* $\mathfrak{M}$ is a subset $\mathfrak{C}_0 \subset \mathfrak{C}$ such that $|C \cap C'| = 2$ for any two distinct circles $C, C' \in \mathfrak{C}_0$. We ask how large such a family $\mathfrak{C}_0$ can be. Our 'cheap' upper and lower bounds are analogues of the corresponding results for Miquelian inversive planes, due to Blokhuis and Bruen [BB].

8.1 Theorem. *$\mathfrak{M}$ has a family of $(3q-1)/2$ doubly intersecting circles.*

Proof. Let $\mathfrak{M}$ be constructed from the cone $X_0^2 = X_1X_2$ in $PG(3,q)$, and let $\mathfrak{C}_0$ consist of the intersections of the cone with the planes $X_3 = 0,\ X_3 = \omega^i X_0,\ X_3 = \omega^i(X_1 - X_0)$, $X_3 = \omega^i(X_2 - X_0)$ for $i = 0, 1, 2, \ldots, (q-3)/2$ where $\langle\omega\rangle = F^\backsim\{0\}$. It is straightforward to check that $\mathfrak{C}_0$ has the required properties. □

Note that the following upper bound in fact holds for arbitrary (not necessarily classical) Laguerre planes (these are defined axiomatically in [KK]).

8.2 Theorem. $|\mathfrak{C}_0| \leq \frac{1}{2}(q^2+1)$.

Proof. Fix a circle $C \in \mathfrak{C}_0$. Counting the number of pairs (P, C') such that $P \in C' \cap C$ and $C \neq C' \in \mathfrak{C}_0$, we have $2(|\mathfrak{C}_0| - 1) \leq (q+1)(q-1)$, from which the result follows. □

Computer searches suggest that the true upper bound for $|\mathfrak{C}_0|$ is much closer to $(3q-1)/2$ than $(q^2+1)/2$. For $q = p^e$ where $p \leq 7$, we obtain a significantly improved upper bound, using the results of Section 7.

8.3 Theorem. $|\mathfrak{C}_0| \leq \binom{(p+7)/2}{4}^e$ *where* $q = p^e$.

Proof. Let (V, Q) be an $O_5(q)$ space, and let $\langle x_0\rangle$ be a singular point of (V, Q). The singular points of the projective 3-space $PG(x_0^\perp)$ form a quadratic cone. Realise $\mathfrak{C}_0$ as the set of intersections of planes $\pi_1, \pi_2, \ldots, \pi_m \subset x_0^\perp$ with this cone. Each $\pi_i^\perp$ is a hyperbolic line in V, containing exactly two singular points, $\langle x_0\rangle$ and (say) $\langle x_i\rangle$. Since $\pi_i \cap \pi_j$ contains two singular points of $x_0^\perp$ whenever $i \neq j$, we see that $\langle x_0, x_i, x_j\rangle^\perp$ is a hyperbolic line, i.e. $-2\delta f(x_0, x_i) f(x_i, x_j) f(x_j, x_0)$ is a nonzero square in F, where $\delta = \mathrm{disc}(Q)$ and $f(x, y)$ is the bilinear form associated to Q (this follows from the proof of Theorem 7.1). It follows that $-2\delta f(x_i, x_j) f(x_j, x_k) f(x_k, x_i)$ is a nonzero square for any 3-subset $\{i, j, k\} \subseteq \{0, 1, 2, \ldots, m\}$, so that $\{\langle x_i\rangle : 0 \leq i \leq m\}$ is a cap in $O_5(q)$ with trivial

two-graph. By Theorem 7.4, we have $m+1 \leq \binom{4+(p-1)/2}{4}^e + 1$ as required. □

For $p = 3, 5, 7$, this gives (approximately) $|\mathfrak{C}_0| \leq q^{1.465}, q^{1.683}, q^{1.827}$ respectively, an improvement over the quadratic upper bound of Theorem 8.2. Unfortunately, however, the new bound is useless for $p \geq 11$; moreover, this approach apparently does not improve upon the quadratic upper bounds for families of doubly intersecting circles in inversive planes.

References

[BLT] L. Bader, G. Lunardon and J. A. Thas, 'Derivation of flocks of quadratic cones', *Forum Math.* **2** (1990), *no. 2,* 163–174.

[Be] H. Bender, 'Endliche zweifach transitive Permutationsgruppen, deren Involutionen keine Fizpunkte haben', *Math. Z.* **104** (1968), 175–204.

[Bl] A. Blokhuis, 'On subsets of $GF(q^2)$ with square differences', Indag. Math. **87** (1984), *no. 4,* 369–372.

[BB] A. Blokhuis and A. A. Bruen, 'The minimal number of lines intersected by a set of $q+2$ points, blocking sets, and intersecting circles', *J. Comb. Theory Ser. A* **50** (1989), *no. 2,* 308–315.

[BM] A. Blokhuis and G. E. Moorhouse, 'Some p-ranks related to orthogonal spaces', submitted to *J. Algeb. Combin.*

[BW] A. E. Brouwer and H. A. Wilbrink, 'Block designs', in *Handbook of Incidence Geometry. Foundations and Buildings',* ed. F. Buekenhout, North-Holland, Amsterdam and New York, 1994.

[Cam] P. J. Cameron, 'Cohomological aspects of two-graphs', *Math. Z.* **157** (1977), 101–119.

[Car] L. Carlitz, 'A theorem on permutations in a finite field', *Proc. Amer. Math. Soc.* **11** (1960), 456–459.

[Ch1] C. Charnes, Ph.D. thesis, Cambridge University.

[Ch2] C. Charnes, 'Quadratic matrices and the translation planes of order 5^2', in *Coding Theory, Design Theory, Group Theory,* ed. D. Jungnickel and S. A. Vanstone, Wiley, New York, 1993, pp. 155–161.

[Cz] T. Czerwinski, 'The collineation groups of the translation planes of order 25', *Geom. Ded.* **39** (1991), 125–137.

[CO] T. Czerwinski and D. Oakden, 'The translation planes of order 25', *J. Comb. Theory Ser. A* **52** (1992), 193–217.

[DGS] P. Delsarte, J. M. Goethals and J. J. Seidel, 'Orthogonal matrices with zero diagonal, II', *Canad. J. Math.* **23** (1971), 816–832.

[D] U. Dempwolff, 'Translation planes of order 27', *Designs, Codes and Cryptography* **4** (1994), 105–121.

[GS] J. M. Goethals and J. J. Seidel, 'Orthogonal matrices with zero diagonal', *Canad. J. Math.* **19** (1967), 1001–1010. Reprinted in [Se2], pp.257–266.

[HT] J. W. P. Hirschfeld and J. A. Thas, *General Galois Geometries,* Oxford Univ. Press, Oxford and New York, 1991.

[Ka1] W. M. Kantor, 'Ovoids and translation planes', *Canad. J. Math.* **34** (1982), *no. 5,* 1195–1207.

[Ka2] W. M. Kantor, 'Some generalized quadrangles with parameters q^2, q', *Math. Z.* **192** (1986), 45–50.

[Ka3] W. M. Kantor, 'Generalized quadrangles, flocks, and BLT sets', *J. Combin. Theory Ser. A* **58** (1991), 153–157.

[KK] H. Karzel and H.-J. Kroll, 'Perspectivities in circle geometries', in: *Geometry—von Staudt's Point of View,* ed. P. Plaumann and K. Strambach, Reidel, Dordrecht, Boston and London, 1981, pp.51–99.

[Kl] P. B. Kleidman, 'The 2-transitive ovoids', *J. Alg.* **117** (1988), *no. 1,* 117–135.

[L] H. Lüneburg, *Translation Planes,* Springer Verlag, Berlin and New York, 1980.

[MR] R. Mathon and G. F. Royle, 'The translation planes of order 49', *Des. Codes and Crypt.,* to appear.

[Mc] B. D. McKay, 'nauty user's guide (version 1.5)', Technical report TR-CS-90-02, Comp. Sci. Dept., Austral. Nat. Univ., 1990.

[Mo] G. E. Moorhouse, 'Ovoids from the E_8 root lattice', *Geom. Ded.* **46** (1993), 287–297.

[Se1] J. J. Seidel, 'A survey of two-graphs', in *Colloquio Internazionale sulle Teorie Combinatorie,* Accademia Nazionale dei Lincei, Roma 1976, pp.481–511. Reprinted in [Se2], pp.146–176.

[Se2] J. J. Seidel, *Geometry and Combinatorics: Selected Works of J. J. Seidel,* ed. R. A. Mathon and D. G. Corneil, Boston, Acad. Press, San Diego and London, 1991.

[SeT] J. J. Seidel and D. E. Taylor, 'Two-graphs, a second survey', in *Algebraic Methods in Graph Theory,* Colloq. Math. Soc. János Bolyai no. 25, ed. L. Lovasz and V. T. Sós, North-Holland, Amsterdam, 1981, pp.689–711. Reprinted in [Se2], pp.231–254.

[Sh] E. Shult, 'Nonexistence of ovoids in $\Omega^+(10,3)$', *J. Comb. Theory Ser. A* **51** (1989), 250–257.

[ShT] E. E. Shult and J. A. Thas, 'm-systems of polar spaces', *J. Comb. Theory Ser. A* **68** (1994), 184–204.

[Ta1] D. E. Taylor, *The geometry of the classical groups*, Heldermann Verlag, Berlin, 1992.

[Ta2] D. E. Taylor, 'Two-graphs and doubly transitive groups', *J. Comb. Theory Ser. A* **61** (1992), 113–122.

[Th1] J. A. Thas, 'Ovoids and spreads of finite classical polar spaces', *Geom. Ded.* **10** (1981), 135–144.

[Th2] J. A. Thas, 'Generalized quadrangles and flocks of cones', *Europ. J. Comb.* **8** (1987), 441–452.